

WE CLAIM:

- 5 1. A method for multiplying an elliptic curve point $Q(x,y)$ by a scalar to provide a point kQ , the method comprising the steps of:
 - a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda \cdot Q$ for all points $Q(x,y)$ on the elliptic curve, and λ is an integer,
 - 10 b) establishing a representation of said scalar k as a combination of components k_i said integer λ
 - c) combining said representation and said point Q to form a composite representation of a multiple corresponding to kQ and
 - d) computing a value corresponding to said point kQ from said composite representation of kQ .
- 15 2. A method according to claim 1 wherein each of said components k_i is shorter than said scalar k .
3. A method according to claim 1 wherein said components k_i are initially selected and subsequently combined to provide said scalar k .
- 20 4. A method according to claim 1 wherein said representation is of the form

$$k_i = \sum_{i=0}^{i=n} k_i \lambda^i \text{ mod } n \text{ where } n \text{ is the number of points on the elliptic curve.}$$
5. A method according to claim 4 wherein said representation is of the form $k_0 + k_1$.
6. A method according to claim 1 wherein said scalar k has a predetermined value and said components k .
- 25 7. A method according to claim 3 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.
8. A method according to claim 7 wherein grouped terms G_i utilized in said simultaneous multiple addition are precomputed.

9. A method according to claim 6 wherein said components k_i are obtained by obtaining short basis vectors (u_0, u_1) of the field F , designating a vector v as $(k, 0)$, converting v from a standard, orthonormal basis to the (u_0, u_1) basis, to obtain fractions f_0, f_1 representative of the vector v , applying said fractions to k to obtain a vector z ,
 5 calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ .
10. A method of generating in an elliptic curve cryptosystem a key pair having an integer k providing a private key and a public key kQ , where Q is a point on the curve,
 10 a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda Q$ for all points $Q(x, y)$ on the elliptic curve, λ is an integer,
 b) establishing a representation of said key k as a combination of components k_i and said integer λ ,
 15 c) combining said representation and said point Q to form a composite representation of a multiple corresponding to the public key kQ and
 d) computing a value corresponding to said key kQ from said composite representation of kQ .
- 20 11. A method according to claim 10 including a method according to any one of claims 2 to 9.